UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/902,583	07/12/2001	Hisao Naitoh	1083.1083	9449

21171 7590 07/18/2006

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/902,583	NAITOH, HISAO	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 April 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on April 19, 2006. Claims 1-18 are currently being considered.

Response to Arguments

2. Applicant's arguments filed April 19, 2006 have been fully considered but they are not persuasive for the following reasons:

Regarding claim 1, the Applicant argues that the Cited Prior Art (CPA), Conklin et al. (U.S. Patent 5,991,881), does not teach "detection of a computer virus in information transmitted from the terminal apparatus to the central apparatus by the installed anti-virus software." This argument is not found persuasive. The CPA discloses a network surveillance system (Figure 2), which is situated on a network and monitors and logs all communications between terminal apparatuses (column 3 lines 36-61). All the packets transmitted between terminal appartuses are also passed through the network surveillance system (column 3 lines 51-56). Therefore, it is asserted that traffic between a central apparatus and a terminal apparatus is monitored and recorded. Furthermore, these recorded logs are examined for possible intrusion patters (column 4 lines 30-34). Therefore, the network surveillance system (central apparatus) detects a virus in information transmitted between the terminal apparatus and the central apparatus.

Furthermore, the Applicant argues that the CPA does not teach "storing a communication history of the terminal apparatus." This argument is not found persuasive. The CPA states that the central apparatus writes a log of the network traffic (column 4 lines 16-29), which is then analyzed for possible intrusion patterns (column 4 lines 30-39). This logging and recording function is seen as analogous to storing a communication history, and therefore, it is asserted that the CPA does teach storing a communication history of the terminal apparatus. Furthermore, the Applicant argues that the CPA does not teach "specifying the time of infection." This argument is not found persuasive. The CPA teaches a continuous monitoring, recording and analyzing process, wherein traffic is recorded and analyzed, and if an intrusion is found, a data structure is formed with a date-time stamp indicating the time of detection (column 5 lines 23-32). This is analogous to the time of infection, and therefore, it is asserted that the CPA does teach specifying a time of infection.

In light of the above arguments, the rejection for the pending claims is respectfully maintained as given below.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-18 are rejected under 35 U.S.C. 102(b) as being anticipated by Conklin et al. (U.S. Patent No. 5,991,881).

Regarding claim 1, Conklin discloses:

A computer virus infection information providing method for detecting a computer virus in information transmitted between a terminal apparatus and a central apparatus and providing infection information concerning the detected computer virus, comprising the steps of:

installing anti-virus software on the central apparatus (column 3 lines 40-46);

storing a communication history of the terminal apparatus (column 4 lines 16-29, 55-60), wherein the network packets traffic is logged;

specifying the time of infection of the terminal apparatus based on the stored communication history in response to a detection of a computer virus in information transmitted from the terminal apparatus to the central apparatus by the installed anti-virus software (column 5 lines 23-32), wherein in the continuous process, the intrusion detection function identifies the network traffic as reportable, will construct a data structure containing a time stamp indicating the time of detection;

transmitting the infection information including the specified time of infection, from the central apparatus to the terminal apparatus (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station; and displaying the transmitted infection information by using the terminal apparatus (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station and is displayed.

Regarding claim 2, Conklin discloses:

A computer virus infection information providing system for detecting a computer virus and providing infection information concerning the detected computer virus, comprising:

a central apparatus (column 2 lines 42-57); and

a terminal apparatus connected to the central apparatus via a communication network (column 2 lines 42-57);

wherein the central apparatus includes a processor capable of performing operations of:

installing anti-virus software (column 3 lines 40-46);

storing a communication history of the terminal apparatus (column 4 lines 16-29, 55-60), wherein the network packets traffic is logged;

specifying the time of infection of the terminal apparatus based on the stored communication history in response to detection of a computer virus in received information transmitted from the terminal apparatus by the installed anti-virus software (column 5 lines 23-32), wherein in the continuous process, the intrusion detection function identifies the network traffic as reportable, will construct a data structure containing a time stamp indicating the time of detection; and transmitting the infection information including the specified time of infection, to the terminal apparatus (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station; and

wherein the terminal apparatus includes a processor capable of performing the operation of:

displaying the transmitted infection information (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station and is displayed.

Regarding claim 11, Conklin discloses:

An infection information providing apparatus for detecting a computer virus in transmitted and received information and providing infection information concerning the detected computer virus, comprising a processor capable of performing operations of:

installing anti-virus software (column 3 lines 40-46);

storing communication history of the information (column 4 lines 16-29, 55-60), wherein the network packets traffic is logged;

specifying the time of infection of a terminal apparatus based on the stored communication history in response to detection of a computer virus in received information by the installed anti-virus software (column 5 lines 23-32), wherein in the continuous process, the intrusion detection function identifies the network traffic as reportable, will construct a data structure containing a time stamp indicating the time of detection; and transmitting the infection information including the specified time of infection, to the outside (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station.

Regarding claim 15, Conklin discloses:

A computer memory product readable by a computer and storing a computer program for detecting a computer virus in transmitted and received information and providing infection information concerning the detected computer virus, the computer program comprising the steps of:

storing a communication history of the information (column 4 lines 16-29, 55-60), wherein the network packets traffic is logged; and

specifying the time of infection of a terminal apparatus based on the stored communication history in response to detection of a computer virus in received information by anti-virus software (column 5 lines 23-32), wherein in the continuous process, the intrusion detection function identifies the network traffic as reportable, will construct a data structure containing a time stamp indicating the time of detection.

Regarding claim 16, Conklin discloses:

A computer virus infection information providing system for detecting a computer virus and providing infection information concerning the detected computer virus, comprising:

a central apparatus (column 2 lines 42-57); and a terminal apparatus connected to the central apparatus via a communication network (column 2 lines 42-57);

wherein the central apparatus includes:

means for installing anti-virus software (column 3 lines 40-46);

means for storing a communication history of the terminal (column 4 lines 16-29, 55-60), wherein the network packets traffic is logged;

means for specifying the time of infection of the terminal apparatus based on the stored communication history in response to detection of a computer virus in information transmitted from the terminal apparatus to the central apparatus by the installed anti-virus software (column 5 lines 23-32), wherein in the continuous process, the intrusion detection function identifies the network traffic as reportable, will construct a data structure containing a time stamp indicating the time of detection; and

means for transmitting the infection information including the specified time of infection to the terminal apparatus (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station; and

wherein the terminal apparatus includes means for displaying the transmitted infection information (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station and is displayed.

Regarding claim 17, Conklin discloses:

An infection information providing apparatus for detecting a computer virus in information transmitted to and received from the outside and providing infection information concerning the detected computer virus, comprising:

means for installing anti-virus software (column 3 lines 40-46);

means for storing a communication history of the information (column 4 lines 16-29, 55-60), wherein the network packets traffic is logged;

means for specifying the time of infection of a terminal apparatus based on the stored communication history in response to detection of a computer virus in the information received from the outside by the installed anti-virus software (column 5 lines 23-32), wherein in the continuous process, the intrusion detection function identifies the network traffic as reportable, will construct a data structure containing a time stamp indicating the time of detection; and

means for transmitting the infection information including the specified time of infection to the outside (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station and is displayed.

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Conklin discloses:

A computer virus infection information providing system according to claim 2, wherein the processor of the central apparatus is further capable of performing an operation of registering the time of find-out which is the time when the computer virus was found out software (column 5 lines 23-32), wherein in the continuous process, the intrusion detection function identifies the network traffic as reportable, will construct a data structure containing a time stamp indicating the time of detection, and

wherein the time of infection is specified based on the stored communication history, the registered time of find-out, and the time of installation of the anti-virus software which is the time when the anti-virus software was installed, when the computer virus is detected by the installed anti-virus software software (column 5 lines 23-32), wherein in the continuous process, the intrusion detection function identifies the network traffic as reportable, will construct a data structure containing a time stamp indicating the time of detection.

Claim 4 is rejected as applied above in rejecting claim 2. Furthermore, Conklin discloses:

A computer virus infection information providing system according to claim 2, wherein the processor of the central apparatus is further capable of performing an operation of specifying the route of infection of the computer virus based on the stored communication history and the time of installation which is the time when the anti-virus software was installed (column 5 lines 26-32), wherein the source and destination IP addresses are recorded; and wherein

the infection information including the specified route of infection and the specified time of infection is transmitted, to the terminal apparatus, when the infection information is transmitted (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station and is displayed.

Claim 8 is rejected as applied above in rejecting claim 2. Furthermore, Conklin discloses:

A computer virus infection information providing system according to claim 2, wherein the processor of the central apparatus is further capable of performing an operation of transmitting advertising information concerning the anti-virus software to the terminal apparatus when a computer virus is detected by the anti-virus software (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station and is displayed.

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Conklin discloses:

An infection information providing apparatus according to claim 11, wherein the processor is further capable of performing an operation of registering the time of find-out which is the time when the computer virus is found out (column 5 lines 23-32), wherein in the continuous process, the intrusion detection function identifies the network traffic as reportable, will construct a data structure containing a time stamp indicating the time of detection, and

the time of infection is specified based on the stored communication history, the registered time of find-out, and the time of installation of the anti-virus software which is the time when the anti-virus software was installed, when a computer virus is detected by the installed anti-virus software (column 5 lines 23-32), wherein in the continuous process, the intrusion detection function identifies the network traffic as reportable, will construct a data structure containing a time stamp indicating the time of detection.

Claim 13 is rejected as applied above in rejecting claim 11. Furthermore, Conklin discloses:

An infection information providing apparatus according to claim 11, wherein the processor is further capable of performing an operation of specifying the route of infection of the computer virus based on the stored communication history and the time of installation which is the time when the anti-virus software was installed (column 5 lines 26-32), wherein the source and destination IP addresses are recorded; and

the infection information including the specified route of infection and the specified time of infection is transmitted to the outside, when the infection information is transmitted (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station and is displayed.

Claim 5 is rejected as applied above in rejecting claim 3. Furthermore, Conklin discloses:

A computer virus infection information providing system according to claim 3, wherein the processor of the central apparatus is further capable of performing an operation of specifying the route of infection of the computer virus based on the stored communication history and the time of installation which is the time when the anti-virus software was installed (column 5 lines 26-32), wherein the source and destination IP addresses are recorded; and wherein

the infection information including the specified route of infection and the specified time of infection is transmitted, to the terminal apparatus, when the infection information is transmitted (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station and is displayed.

Claim 6 is rejected as applied above in rejecting claim 3. Furthermore, Conklin discloses:

A computer virus infection information providing system according to claim 3, wherein the processor of the central apparatus is further capable of performing an operation of transmitting the installed anti-virus software to a predetermined terminal apparatus, wherein the processor of the terminal apparatus is further capable of performing operations of:

installing the transmitted anti-virus software (column 3 lines 40-46);

storing an execution history of the installed anti-virus software (column 4 lines 16-29, 55-60), wherein the network packets traffic is logged; and

transmitting the stored execution history to the central apparatus when a computer virus is detected by the anti-virus software (column 4 line 45 – column 5 line 21), and wherein the processor of the central apparatus is further capable of performing the operations of:

specifying the time of infection based on the transmitted execution history and the registered time of find-out (column 5 lines 23-32), wherein in the continuous process, the intrusion detection function identifies the network traffic as reportable, will construct a data structure containing a time stamp indicating the time of detection;

specifying the route of infection of the computer virus based on the transmitted execution history (column 5 lines 26-32), wherein the source and destination IP addresses are recorded; and

transmitting the infection information including the specified time of infection and the specified route of infection, to the terminal apparatus (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station and is displayed.

Claim 7 is rejected as applied above in rejecting claim 4. Furthermore, Conklin discloses:

A computer virus infection information providing system according to claim 4, wherein the processor of the central apparatus is further capable of performing an operation of transmitting the installed anti-virus software to a predetermined terminal apparatus, wherein the processor of the terminal apparatus is further capable of performing operations of:

installing the transmitted anti-virus software (column 3 lines 40-46);

storing an execution history of the installed anti-virus software (column 4 lines 16-29, 55-60), wherein the network packets traffic is logged; and

transmitting the stored execution history to the central apparatus when a computer virus is detected by the anti-virus software (column 4 line 45 – column 5 line 21), and wherein

the processor of the central apparatus is further capable of performing a operations of:

specifying the time of infection based on the transmitted execution history and the registered time of find-out (column 5 lines 23-32), wherein in the continuous process, the intrusion detection function identifies the network traffic as reportable, will construct a data structure containing a time stamp indicating the time of detection;

specifying the route of infection of the computer virus based on the transmitted execution history (column 5 lines 26-32), wherein the source and destination IP addresses are recorded; and

transmitting the infection information including the specified time of infection and the specified route of infection, to the terminal apparatus (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station and is displayed.

Claim 9 is rejected as applied above in rejecting claim 3. Furthermore, Conklin discloses:

A computer virus infection information providing system according to claim 3, wherein the processor of the central apparatus is further capable of performing an operation of transmitting advertising information concerning the anti-virus software to the terminal apparatus when a computer virus is detected by the anti-virus software (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station and is displayed.

Claim 10 is rejected as applied above in rejecting claim 4. Furthermore, Conklin discloses:

A computer virus infection information providing system according to claim 4, wherein the processor of the central apparatus is further capable of performing an operation of transmitting advertising information concerning the anti-virus software to the terminal apparatus when a computer virus is detected by the anti-virus software (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station and is displayed.

Claim 14 is rejected as applied above in rejecting claim 12. Furthermore, Conklin discloses:

An infection information providing apparatus according to claim 12, wherein the processor is further capable of performing an operation of specifying the route of infection of the computer virus based on the stored communication history and the time of installation which is the time when the anti-virus software was installed (column 5 lines 26-32), wherein the source and destination IP addresses are recorded, and

the infection information including the specified route of infection and the specified time of infection is transmitted, to the outside, when the infection information is transmitted (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station and is displayed.

Regarding claim 18, Conklin discloses:

A computer virus infection information providing method for detecting a computer virus in information transmitted between a client and a server and providing infection information concerning the detected computer virus, comprising:

installing anti-virus software on the server apparatus (column 3 lines 40-46);

detecting the virus and specifying a time of detection (column 5 lines 23-32), wherein in the continuous process, the intrusion detection function identifies the network traffic as reportable, will construct a data structure containing a time stamp indicating the time of detection;

storing a communication history of the client apparatus software (column 4 lines 16-29, 55-60), wherein the network packets traffic is logged;

specifying a time of infection based on the time of detection and the stored communication history when the virus is detected by the installed anti-virus software (column 5 lines 23-32), wherein in the continuous process, the intrusion detection function identifies the network traffic as reportable, will construct a data structure containing a time stamp indicating the time of detection;

transmitting the infection information including the specified time of infection, from the server to the client (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station and is displayed; and

displaying the transmitted infection information at the client (column 5 lines 47-61, column 7 lines 17-23), wherein a time-stamped alert message is sent to the console or a management station and is displayed.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-273-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA
07/08/2006

07/09/2006